(1) group under modulo-11 addition
$\{0, 1, 2, 3, \ldots 8, 9, 10\}$

(2) Group under modulo-11 multiplication
$\{1, 2, 3, \ldots 8, 9, 10\}$

(3) $\{1, 2, \ldots m-1\}$

Since m is not a prime, it can be factored as the product of two integers 'a' and 'b'.

$m = a \cdot b$

with $1 < a, b < m$, it is clear that both a and b are in the set $\{1, 2, \ldots m-1\}$.

consider the modulo-m multiplication of a & b

$a \boxdot b$ modulo m

$=$ m modulo m

$= 0$

$\Rightarrow a \boxdot b = 0$, since '0' is not an element of set $\{1, 2, \ldots m-1\}$

the set is not closed under the modulo-m multiplication and hence can not be a group.

(4) multiplicative group under modulo-11 multiplication

is {1, 2, 3 . . . 10}

An element in a group is called generator (2, 6, 7, 8) of that, if all other elements of that group can be generated by raising it to different powers and taking modulo-11 operation

We can check that elements 2, 6, 7, 8 satisfy above condition

(5)

$\{\overset{8^1}{8}, \overset{8^2}{12}, \overset{8^3}{5}, \overset{8^4}{1}\}$

for.

1*H = {8, 12, 5, 1} ✓

2*H = {3, 11, 10, 2} ✓

3*H = {11, 10, 2, 3}

4*H = {6, 9, 7, 4} ✓

5*H = {1, 8, 12, 5}

6*H = {9, 7, 4, 6}.

7*H = {4, 6, 9, 7}

8*H = {12, 5, 1, 8}

9*H = {7, 4, 6, 9}

10*H = {2, 3, 11, 10}

11*H = {10, 2, 3, 11}

12*H = {5, 1, 8, 12}

6). Condition (ii) says that every element of H has an inverse in H. Conditions (i) and (ii) ensure that the identity element of G is also in H. Because the elements in H are elements in G, the associative condition on $*$ holds automatically. Hence, H satisfies all the conditions of a group and is a subgroup of G.

7) i) The proof is based on the fact that all the elements in the subgroup H are distinct. Consider the coset $a * H = \{a*h : h \in H\}$ with $a \in G$. Suppose two elements, say $a*h$ and $a*h'$, in $a*H$ are identical, where h and h' are two distinct elements in H. Let a^{-1} denote the inverse of a with respect to the binary operation $*$. Then,

$$a^{-1}*(a*h) = a^{-1}*(a*h')$$

$$(a^{-1}*a)*h = (a^{-1}*a)*h'.$$

$$e*h = e*h'.$$

$$h = h'.$$

This result is a contradiction to the fact that all the elements of H are distinct. Therefore no two elements in a coset are identical.

ii) Let $a*H$ and $b*H$ be two distinct cosets of H, with a and b in G. Let $a*h$ and $b*h'$ be two elements in $a*H$ and $b*H$, respectively. Suppose

$a*h = b*h'$. Let h^{-1} be the inverse of h. Then

$$(a*h)*h^{-1} = (b*h')*h^{-1}$$

$$a*(h*h^{-1}) = b*(h'*h^{-1})$$

$$a*e = b*h''$$

$$a = b*h''$$

where $h'' = h'*h^{-1}$ is an element H. The equality $a = b*h''$ implies that

$$a*H = (b*h'')*H.$$

$$= \{(b*h'')*h : h \in H\}$$

$$= \{b*(h''*h) : h \in H\}$$

$$= \{b*h''' : h''' \in H\}$$

$$= b*H$$

This result says that $a*H$ and $b*H$ are identical, which is a contradiction to the given condition that $a*H$ and $b*H$ are two distinct cosets of H. Therefore, no two elements in two distinct cosets of H are identical.

8.

Property I For every element a in a field, $a \cdot 0 = 0 \cdot a = 0$.

Proof. First, we note that

$$a = a \cdot 1 = a \cdot (1 + 0) = a + a \cdot 0.$$

Adding $-a$ to both sides of the preceding equality, we have

$$-a + a = -a + a + a \cdot 0$$
$$0 = 0 + a \cdot 0$$
$$0 = a \cdot 0.$$

Similarly, we can show that $0 \cdot a = 0$. Therefore, we obtain $a \cdot 0 = 0 \cdot a = 0$. **Q.E.D.**

Property II For any two nonzero elements a and b in a field, $a \cdot b \neq 0$.

Proof. This is a direct consequence of the fact that the nonzero elements of a field are closed under multiplication. **Q.E.D.**

Property III $a \cdot b = 0$ and $a \neq 0$ imply that $b = 0$.

Proof. This is a direct consequence of Property II. Q.E.D.

Property IV For any two elements a and b in a field,

$$-(a \cdot b) = (-a) \cdot b = a \cdot (-b).$$

Proof. $0 = 0 \cdot b = (a + (-a)) \cdot b = a \cdot b + (-a) \cdot b$. Therefore, $(-a) \cdot b$ must be the additive inverse of $a \cdot b$, and $-(a \cdot b) = (-a) \cdot b$. Similarly, we can prove that $-(a \cdot b) = a \cdot (-b)$. Q.E.D.

Property V For $a \neq 0$, $a \cdot b = a \cdot c$ implies that $b = c$.

Proof. Because a is a nonzero element in the field, it has a multiplicative inverse, a^{-1}. Multiplying both sides of $a \cdot b = a \cdot c$ by a^{-1}, we obtain

$$a^{-1} \cdot (a \cdot b) = a^{-1} \cdot (a \cdot c)$$
$$(a^{-1} \cdot a) \cdot b = (a^{-1} \cdot a) \cdot c$$
$$1 \cdot b = 1 \cdot c.$$

Thus, $b = c$. Q.E.D.

(9) $G = \{0, 1, 2, 3, \ldots 31\}$ under modulo-32 addition

$H = \{0, 4, 8, 12, 16, 20, 24, 28\}$

$\forall a \in H, \Rightarrow a \in G,$

Clearly $H \subset G$ { H is a subset of G }

We know that a subset (H) of a group becomes subgroup if it satisfies

(i) closed under the operation defined on 'G'

(ii) for any element 'a' in H, the inverse of 'a' is also in H.

Closed under modulo-32

$4K, 4L \in H$ $\quad K, L \in \{0, 1, 2 \ldots 7\}$

consider $(4K + 4L)$ modulo 32

$= 4\{(K+L) \bmod 8\}$

$\in H,$

so H is closed under modulo-32

for inverse

let $4K \in H$ $\quad K \in \{0, 1, 2 \ldots 7\}$

inverse is $32 - 4K$

$4(8-K) \in H,$

so inverse also exists in H,

so H forms a subgroup in G

Question-11: Let S be a nonempty subset of a vector space V over a field F. Then, S is a subspace of V if the following conditions are satisfied:

i. For any two vectors $\mathbb{u}$ and $\mathbb{v}$ in S, $\mathbb{u} + \mathbb{v}$ is also a vector in S.
ii. For any element a in F and any vector $\mathbb{u}$ in S, $a \cdot \mathbb{u}$ is also in S.

Proof. Conditions (i) and (ii) simply say that S is closed under vector addition and scalar multiplication of V. Condition (ii) ensures that for any vector $\mathbb{v}$ in S its additive inverse $(-1) \cdot \mathbb{v}$ is also in S. Then, $\mathbb{v} + (-1) \cdot \mathbb{v} = \mathbb{0}$ is also in S. Therefore, S is a subgroup of V. Because the vectors of S are also vectors of V, the associative and distributive laws must hold for S. Hence, S is a vector space over F and is a subspace of V. Q.E.D.

(13)

$2x^4 + x^2 - 2$

$3x^2+1 \overline{) x^6 + 3x + 2} ($

$6x^6 + 2x^4$

$-5x^6 - 2x^4 + 3x + 2$

$3x^4 + x^2$

$-5x^4 - x^2 + 3x + 2$

$-6x^2 - 2$

$5x^2 + 3x + 4$

quotient

$2x^4 + x^2 - 2$ & $3x + 4$ ← remainder

EE5160 – Pr Set-2

(1)

GF(8) using x^3+x+1;

(a) say 'α' is a root of x^3+x+1

$\Rightarrow \alpha^3+\alpha+1=0$

$\Rightarrow \alpha^3 = 1+\alpha$

and $\alpha^4 = \alpha^3\cdot\alpha = \alpha+\alpha^2$

	1	α	α^2
0	0	0	0
1	1	0	0
α	0	1	0
α^2	0	0	1
α^3	1	1	0
α^4	0	1	1
α^5	1	1	1
α^6	1	0	1

$(\alpha^7=1)$

(b) Let 'β' be root of x^3+x^2+1

$\Rightarrow \beta^3 = \beta^2+1$

	1	β	β^2
0	0	0	0
1	1	0	0
β	0	1	0
β^2	0	0	1
β^3	1	0	1
β^4	1	1	1
β^5	1	1	0
β^6	0	1	1

$\beta^7=1$

(C) now let us find which power of 'β' satiesfies the first equation x^3+x+1,

we can see that $(\beta^3)^3+\beta^3+1 \Rightarrow \beta^7\cdot\beta^2+\beta^3+1$

$\Rightarrow \beta^2+\beta^3+1=0$.

so β^3 is a root of x^3+x+1,

$\alpha \leftrightarrow \beta^3$ is an isomorphism between the two fields

We know that,

two fields F & G are said to be isomorphic if there is a one to one mapping from F onto G, which preserves addition and multiplication

element 1 + element α^2 = element α^6

$1+\alpha^2 = \alpha^6$

Substituting $\alpha = \beta^3$

$1+(\beta^3)^2 = (\beta^3)^6$

$\Rightarrow 1+\beta^6 = \beta^{18}$

$\Rightarrow 1+\beta^1+\beta^2 = \beta^{14}.\beta^4$

~~$\beta^4 = \beta^4$~~

$\Rightarrow \beta^4 = \beta^4$,

(2)

$\beta \in GF(q^m)$

$\Rightarrow \beta^{q^m - 1} = 1$ ——— (1)

given that $\beta^{q^e} = \beta$

$\Rightarrow \beta^{q^e - 1} = 1$ ——— (2)

from (1) & (2) $e < m$ (smallest e)

$q^e - 1 \mid q^m - 1$ (refer Theorem)

let $m = Qe + R$ $\quad 0 \leq R < e$

$$\frac{q^m - 1}{q^e - 1} = \frac{q^{Qe+R} - 1 + q^R - q^R}{q^e - 1}$$

$$= q^R \frac{q^{Qe} - 1}{q^e - 1} + \frac{q^R - 1}{q^e - 1}$$

$(q^{Qe} - 1)$ is always divisible by $q^e - 1$

$(\because (x^n - 1) = (x-1)(x^{n-1} + x^{n-2} + \cdots + 1))$

the last term is less than 1 and so is an integer iff $R = 0$

i.e $e \mid m$

[Thm 2.9: Let a be a nonzero element in a finite field $GF(q)$. Let n be the order of a. Then n divides $q-1$.]

Problem Set-2

1) a) Consider the Galois field $GF(2^5)$ given by Table 2.10. $\beta = \alpha^5$, The conjugates of β are

$$\beta^2 = \alpha^{10}, \quad \beta^{2^2} = \alpha^{20}, \quad \beta^{2^3} = \alpha^9, \quad \beta^{2^4} = \alpha^{18}$$

The minimal polynomial of $\beta = \alpha^5$ is then

$$\phi(X) = (X+\alpha^5)(X+\alpha^{10})(X+\alpha^{20})(X+\alpha^9)(X+\alpha^{18})$$

$$\phi(x) = x^5 + x^4 + x^2 + x + 1$$

b) Let $\beta = \alpha^7$

$$\beta^2 = \alpha^{14}, \quad \beta^{2^2} = \alpha^{28}, \quad \beta^{2^3} = \alpha^{25}, \quad \beta^{2^4} = \alpha^{19}$$

The minimal polynomial of $\beta = \alpha^7$ is then

$$\phi(x) = (x+\alpha^7)(x+\alpha^{14})(x+\alpha^{28})(x+\alpha^{25})(x+\alpha^{19})$$

$$\phi(x) = x^5 + x^3 + x^2 + x\ 1$$

(5) let us say $b \in GF(q)$ and $order(b) = n$,

b is non zero & b not unity

since $b \in GF(q)$, $n \leq q-1$,

We know that order divides q-1

$\Rightarrow n | q-1$,

Given that 'q-1' is prime.

so $n = q-1$,

so every nonzero element of GF(q) not equal to the unit element is primitive.